新一代對稱式密碼學演算法於智慧卡上的具體實現

楊中皇[1]、蔡金鳳[2]

[1]國立高雄第一科技大學 資訊管理系
http://www.nkfust.edu.tw/~chyang/
E-mail: chyang@ccms.nkfust.edu.tw

[2]輔英技術學院
E-mail: zoee@mail.fy.edu.tw

摘要

去年美國政府機構 NIST 正式宣布選用 Rijndael 密碼學演算法作為 AES (Advanced Encryption Standard)，且已於今年二月底公布 AES 草案，逐步取代行之已久之 DES (Data Encryption Standard)。除了美國 NIST 的 AES 計畫，歐洲也正在進行 NESSIE 計畫，日本也有 CRYPTREC 計畫，皆正在評估新一代的密碼學演算法。

本研究是在探討智慧卡內部之對稱式密碼學演算法的效率及韌體組合語言程式具體實現。我們實現 AES 及歐洲 NESSIE 計畫與日本 CRYPTREC 計畫的部分候選密碼學演算法，包括 RSA 公司的 RC6, NTT 公司的 FEAL-32X, 以及 NTT 暨三菱公司的 Camellia。除了在內含 H8/300 八位元中央處理器的日立公司 H8/3113 智慧卡晶片內部進行密碼學演算法的具體實現，本研究也同時在內含 6805 八位元中央處理器的摩托羅拉公司 MC68HC705B16 微控制器上進行 AES 等演算法的具體實現，並開發低成本的資訊安全硬體雛型設備。

我們具體實現結果顯示在八位元 6805 或 H8/300 中央處理器的智慧卡上 AES-128 加密執行效率大約為 DES 的４倍，Camellia 與 AES 加密執行效率在伯仲之間，而 RC6 加密執行效率則比 AES 慢約 10 倍。AES 金鑰安排(key schedule)顯著地優於其他演算法，AES-128 於 MC68HC705B16 加密速度可達 30 Kbits/秒，而於 H8/3113 加密速度更可達 76 Kbits/秒。

關鍵詞：*IC 卡，智慧卡，密碼學，對稱式，保密，DES，AES，Camellia，FEAL。*

壹、 前言

隨著網路技術的快速發展及應用，IC 卡[1-2]在業界的應用日趨廣泛。例如：目前應用最多且被金融界視為塑膠貨幣的 IC 金融卡、由中國信託商業銀行與文化大學合作結合金融卡與學生證功能的學生證智慧卡、中華電信推出之 IC 通話卡、偉登資訊與十大書坊聯合推出租書 IC 卡的計劃、中央健保局在澎湖試辦的健保 IC 卡、中國信託商業銀行與中國石油公司和台北捷運局等合作推出之卡票合一儲值金融卡、運用在停車場管理及收費的 IC 智慧卡、以及政府正在推行之健保 IC 卡・・・等等。由以上實例可知 IC 卡的應用日趨重要亦是未來發展的趨勢。

IC 卡與目前常用的磁條卡比較起來具有難以偽造與記憶體容量較高的優點，然而價位也較高。IC 卡又可分為記憶型(例如電話 IC 卡)與智慧型(例如金融 IC 卡)，前者安全性較差且不適合用於電子商務等，後者則價位較高且可多用途如安全電子郵件系統及網路安全下單系統。然而從我們多年使用國外廠商所開發 IC 卡應用系統的經驗中，常見的問題便是廠商技術支援不足及價格偏高。而且廠商通常僅能提供較不安全的密碼學演算法，例如 56 位元 DES (Data Encryption Standard) [3]，而多半無法提供較高安全功能如 Triple-DES 或在使用上有所限制。

本研究是將對稱式(symmetric) 密碼學演算法[4]具體實現於智慧卡。近年來新一代對稱式密碼學演算法一一浮現。例如 2000 年 10 月美國政府機構 NIST 正式宣布[5]選用 Rijndael 演算法作為 AES (Advanced Encryption Standard) [6]，且已於今年二月底公布 AES 草案[7]，，逐步取代行之已久之 DES。除了美國 NIST 的 AES 計畫，歐洲也正在進行 NESSIE

[8]計畫，評估新一代的密碼學演算法，目前日本也有類似的 CRYPTREC [9]計畫。本研究除了進行 AES 的具體實現外，我們也評估 NESSIE 及 CRYPTREC 的部分候選密碼學演算法，包括 RSA 公司的 RC6 [10] ，NTT 公司的 FEAL-NX [11]，以及 NTT 暨三菱公司的 Camellia [12]。

我們以 H8/3113 智慧卡晶片[13]進行具體實現。但由於智慧卡需開模(masking)且訂購數量至少上千單位，所費不貲；且新型的智慧卡內部有數學運算加速器，可用於高安全性加解密應用，也因而此型智慧卡的發展系統及晶片皆受到傳統的輸出管制。所以我們也於具備八位元 6805 中央處理位元之 MC68HC705B16 [14]單晶片微處理器(microcontroller)進行具體實現。此單晶片內含 E^2PROM 可動態儲存金鑰而不需開模，我們正以 MC68HC705B16 開發低製造成本的資訊安全硬體雛型設備。此雛型設備不但可提供用戶端安全保密或伺服器安全保密亦可用於以對稱式演算法為基礎的安全網路通信應用。

無可諱言地，智慧卡的使用是未來趨勢，一張智慧卡不僅可用做身份識別，也可提供門禁管制、電子郵件(電子公文)、圖書借還書、成績輸入與查詢等功能。這使得攸關 IC 卡安全性的密碼學演算法日行重要。本研究於智慧卡上具體實現與評估 AES 等新一代對稱式密碼學演算法，同時開發低成本資訊安全雛形軟硬體設備，以使政府大力推行智慧卡時能掌握關鍵性密碼學演算法具體實現的技術。

貳、6805 與 H8/300

我們以日立公司新型 H8/3113 智慧卡晶片及微處理器 MC68HC705B16 進行 AES、Camellia 等密碼學演算法的具體實現，在此我們簡單描述這兩硬體裝置的特性。H8/3113(晶片 IC 內部結構如圖 1)提供八位元 RISC 式的 H8/300 微處理機，32K 位元組(byte)唯讀記憶體(ROM)，16K 位元組可讀寫唯讀記憶體(E^2PROM)，2.5K 位元組隨機存取記憶體(RAM)，以及 1024 位元大數乘法加速器(coprocessor)，適合對稱性與非對稱性密碼學演算法的具體實現。晶片的唯讀記憶體區域是用來儲存作業系統程式和儲存 AES 密碼運算法或其他固定的應用程式；可程式唯讀記憶體區域是用來儲存個人化的資料(如私密金匙、公開金匙憑證)或其他易更動的應用程式；隨機存取記憶體區域則是供暫時性運算變數資料儲存用。H8/3113 中央處理器僅是八位元，RAM 僅有 2.5K 位元組（其中 0.5K 位元組供乘法加速器用），程式大小亦有限制；這使得晶片程式的開發必須以組合語言為主，以便有效地利用有限的資源。

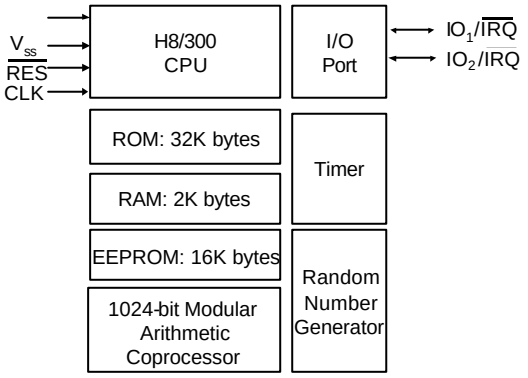

圖 1：H8/3113 智慧卡晶片內部結構圖

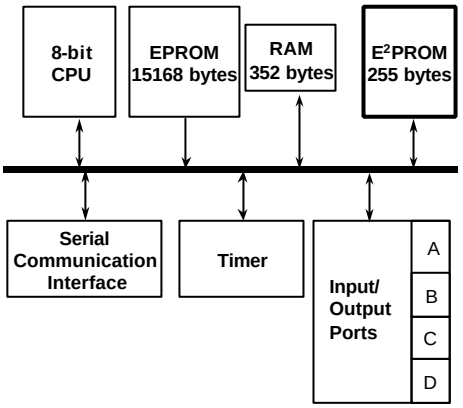

圖 2：MC68HC705B16 微處理器內部結構圖

MC68HC705B16 內部結構如圖 2，提供八位元的 6805 微處理機，15K 位元組 ROM，256 位元組 E^2PROM，352 位元組 RAM，及四組輸出入阜。但由於 MC68HC705B16 記憶體 RAM 很少，僅有兩個 176 位元組不連續區域共 352 位元組，這使得程式撰寫比 H8/3113 更為不易。MC68HC705B16 單晶片內含 E^2PROM 可動態儲存金鑰而不需開模，甚至有一次燒錄(one-time programmable)裝置可由使用者自行燒錄韌體，且單價便宜。在兩種不同架構的八位元中央處理器上實現密碼學演算法，可讓我們進一步瞭解演算法的執行效率，同時單晶片微處理器不像智慧卡晶片有輸出的管制。

參、具體實現

Rijndael 發明者曾於 8051 及 6808 進行具體實現[6]，Keating [15]以高階語言軟體模擬 Rijndael 於 6805 的加解密速度，Hachez 等[16]則具體實現 Rijndael 於 ARM 智慧卡。我們捨高階語言而以組合語言撰寫程式來提高執行速度。本研究將只探討 128 位元(16 位元組)長度之加解密金鑰，因為這最有可能取代 Triple-DES，且適用於我們的 H8/3113 與 MC68HC705B16 平台。

首先我們從分析 AES 等新一代對稱式密碼學演算法之金鑰安排(key schedule)與加解密(encryption/decryption)過程著手。金鑰安排會將輸入之 16 位元組加解密金鑰予以擴張處理成 80 位元組(FEAL-32X)或 176 位元組(AES 及 RC6)或 208 位元組(Camellia)回合金鑰(round key)。這在 H8/3113 是沒問題的，因為它有 2.5K 位元組的 RAM 動態記憶體。然而在 MC68HC705B16 上，僅有 352 位元組的 RAM，且 RAM 分成速度不等之不連續兩部分，便得思考如何擺放回合金鑰以提昇效率。同時 RAM 要保留某些區域給作業系統用。

NIST 評選比利時密碼學家所發明的 Rijndael [6]為 AES 時考慮了安全性、效能、效率、容易實做及有彈性。Rijndael 每回合的轉換沒有 Feistel 結構。反而，回合是數個可逆的轉換所組成，稱作層(layers)。我們實現的 128 位元金鑰與 128 位元明文 AES 的加密過程約如圖 3 所示。金鑰先經計算找出 11 組 128 位元的回合鑰(round key)。明文則經 AddRoundKey（須用到回合鑰）、ByteSubstitution、RotateRow、及 MixColumn 等層的轉換。

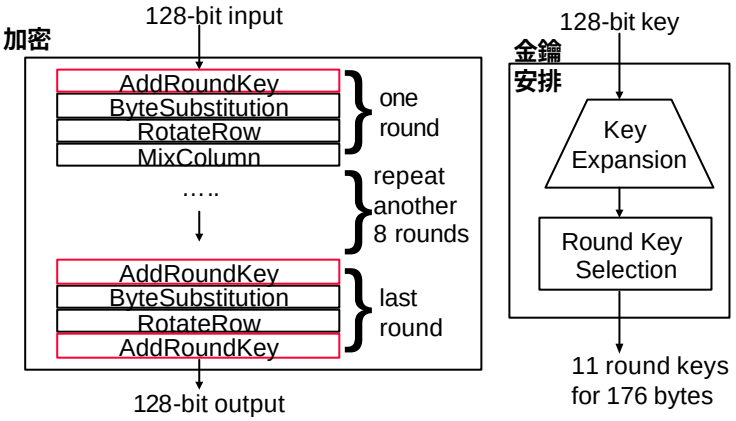

圖 3：AES 加密

FEAL-NX [11]是日本電信電話公司(NTT)改良舊有 FEAL 演算法，金鑰長度可為 64 位元或 128 位元，而其中 N 代表回合(round)數。我們實現 128 位元金鑰的 FEAL-32X。

Camellia [12]是日本 NTT 與三菱公司(Mitsubishi)共同設計的加解密演算法。我們實現的 128 位元金鑰 Camellia 的加密過程約如圖 4 所示。

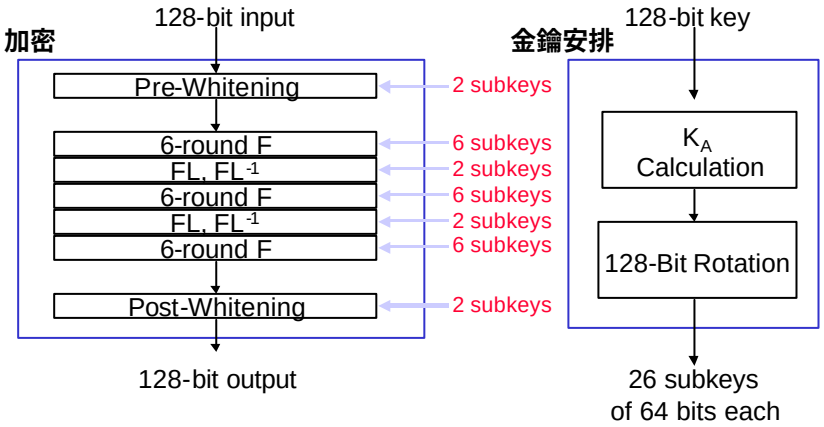

圖 4：Camellia 加密

RC6 [13]則是美國 RSA Data Security, Inc.設計的密碼學演算法，加解密過程與金鑰安排簡潔很容易描述。我們實現的 128 位元金鑰 RC6 的加密過程約如圖 5 所示。

```
B = B + S[ 0 ]
D = D + S[ 1 ]

for i = 1 to 20 do {
   t = ( B x ( 2B + 1 ) ) <<< 5
   u = ( D x ( 2D + 1 ) ) <<< 5
   A = ( ( A ? t ) <<< u ) + S[ 2i ]
   C = ( ( C ? u ) <<< t ) + S[ 2i + 1 ]
   (A, B, C, D) = (B, C, D, A) }

A = A + S[ 42 ]
C = C + S[ 43 ]
```

金鑰安排

```
Subkey [0] = 0xb7e15163;
for (i = 1; I  < 44; ++i)
   Subkey [i] = Subkey [i-1]+0x9e3779b9;
A = B = i = j = 0;
for (count = 132; --count >= 0;)
   A = A + Subkey [i]+B;
   Subkey [i] = A = ROTL(A, 3);
   B = Key [j] + (t = A+B);
   Key [j] = B = ROTL(B, t);
   if (++i == 44)  i = 0;
   if (++j == 4)    j = 0;
```

圖 5：RC6 加密

在進行效率評估時，我們需要在公平的基礎下實施。主要是在接近相同大小的唯讀記憶體(ROM)下做比較。計算 ROM 的大小包括程式碼與所用到的表格（例如 Sbox），而以我們過去的經驗每種對稱式密碼學演算法大約使用 2.5K 位元組。當然同一種演算法越大的 ROM 通常可加快執行速度，但以現行一般智慧卡 16K 至 32K 位元組的 ROM，我們應避免耗費超過 4K 位元組的 ROM 於某種演算法上。

我們於智慧卡晶片 H8/3113 及 MC68HC705B16 微控制器上開發韌體。附錄一顯示我們撰寫的 AES 程式以日立公司智慧卡硬體模擬器及摩托羅拉公司硬體模擬器執行之實際結果。限於篇幅，更詳盡的 AES、FEAL-32X、Camellia、RC6 硬體模擬執行資料請參見 http://www.nkfust.edu.tw/~chyang/isc2001/.

表一：128 位元金鑰之 AES、FEAL-32X、Camellia、RC6 於 MC68HC705B16 執行效率

演算法	金鑰安排(key schedule)時間	加密時間 (每個區塊)	加密處理速度
AES-128	0.95 ms 2000 cycles	4.3 ms 9000 cycles	30 Kbits/s
FEAL-32X	2.2 ms 4700 cycles	3.1 ms 6500 cycles	20.7 Kbits/s
Camellia	3.5 ms 7500 cycles	4.7 ms 9900 cycles	27 Kbits/s
RC6	36 ms 76200 cycles	NA	NA

表二：128位元金鑰之AES與Camellia於H8/3113執行效率

演算法	金鑰安排時間	加密時間 (每個區塊)	加密處理速度
AES-128	0.43 ms 1080 cycles	1.67 ms 4180 cycles	76 Kbits/s
Camellia	0.95 ms 2380 cycles	1.64 ms 4100 cycles	78 Kbits/s

初步實現結果整合如表一及表二所示，其中我們假設MC68HC705B16晶片內部時鐘(clock)為允許之 2.1MHz 而 H8/3113 晶片內部時鐘假設為 5MHz。當程式佔用的記憶體差不多相同

2.5K 位元組時，AES 大約比我們過去具體實現的 DES 速度快約 4 倍。同時由於 128 位元金鑰之 AES 有 3.4 x 10^{38} 可能的金鑰選擇遠較 56 位元 DES 有 7.2 x 10^{16} 可能的金鑰選擇為大，且截至目前為止並無有效攻擊方式，故 AES 除了速度較快外也遠較 DES 安全。 Camellia 的加密速度與 AES 不相上下但金鑰安排(key schedule)較慢。RC6 則遠較 AES 慢太多，除非安全上未來能優於 AES 否則 RC6 並不適合於八位元中央處理器上使用。FEAL-32X 則程式碼較小，速度中等。

肆、金鑰安排

上述新一代加解密演算法的金鑰安排方式大不相同，而金鑰安排的安全性更不易評估[17]。從我們具體實現的經驗顯示 AES 於八位元處理器上確實比其他演算法有效率，尤其在金鑰安排的執行時間更是顯著優於其他演算法。RC6 的金鑰安排流程如圖 5 所示，非常容易描述。然而在八位元平台上 RC6 金鑰安排相較於 AES 時速度極慢，這主要由於它須進行 132 次輸入金鑰值與子金鑰(subkey)值的更新與不定長度的旋轉，如圖 6 所示，而記憶體的讀寫時間是不可忽視的。

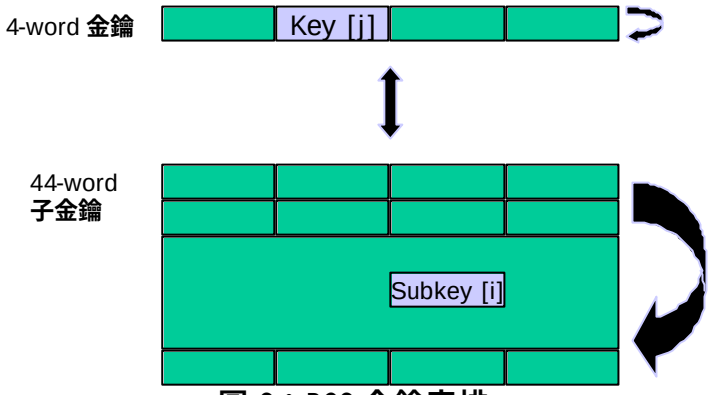

圖 6：RC6 金鑰安排

AES 的金鑰安排在八位元平台則能有效地具體實現。以 AES-128 為例，16 位元組的金鑰將擴展成為 176 位元組的回合金鑰(round key) 。設以 K[0]至 K[175]代表 176 位元組的回合金鑰，則 K[0]至 K[15]內含輸入金鑰值，其他每個位元組的回合金鑰值可依下列計算方式求得：

$$K[16] = K[0] \oplus Sbox(K[13]) \oplus Rcon1$$
$$K[17] = K[1] \oplus Sbox(K[14])$$
$$K[18] = K[2] \oplus Sbox(K[15])$$
$$K[19] = K[3] \oplus Sbox(K[12])$$
$$K[20] = K[16] \oplus K[4]$$
$$K[21] = K[17] \oplus K[5]$$
$$K[22] = K[18] \oplus K[6]$$
$$K[23] = K[19] \oplus K[7]$$
$$K[24] = K[20] \oplus K[8]$$
$$\cdots\cdots\cdots\cdots$$

而我們可以安排如下的計算順序，便能減少記憶體的讀寫。

$$K[16] \oplus K[20] \oplus K[24] \oplus \cdots$$
$$K[17] \oplus K[21] \oplus K[25] \oplus \cdots$$
$$K[18] \oplus K[22] \oplus K[26] \oplus \cdots$$
$$K[19] \oplus K[23] \oplus K[27] \oplus \cdots$$
$$\cdots\cdots\cdots\cdots$$

伍、結論

本研究於智慧卡上具體實現與評估 AES、Camellia、FEAL-32X、RC6 等新一代對稱式密碼學演算法。金鑰 128 位元長度的 AES 於八位元智慧卡或微處理器上加密速度至少比 DES 快四倍，且安全性亦遠較 56 位元金鑰的 DES 強，未來勢必逐漸取代 DES 或 Triple-DES。無可諱言地，IC 卡的使用是未來趨勢，一張智慧卡不僅可做為身份識別用，也可提供門禁管制、電子公文、網路報稅等功能。這使得攸關 IC 卡安全性的密碼學演算法日行重要。本計畫之主要目的在具體實現與評估 IC 卡內部對稱式密碼學演算法，以使政府大力推行 IC 卡時能掌握關鍵性密碼學演算法具體實現的技術。

致謝

本研究獲得國科會計畫（NSC 89-2213-E-327-002）的經費補助，特此致謝。同時感謝 NTT 公司 Kazumaro Aoki 於 Camellia 演算法具體實現的協助及第十一屆全國資訊安全會議匿名論文審查委員對本篇論文的建議。

參考文獻

[1]. W. Rankl, W. Effing, R. Wolfgang， *Smart Card Handbook*，John Wiley & Sons, 1997.

[2]. ISO 7816 Part 1 to 6: *Identification Cards – Integrated Circuit(s) Cards with Contacts*, 1987 to 1996.

[3]. National Institute of Standards and Technology, Federal Information Processing Standard (FIPS) 46-3, *Data Encryption Standard*, October 25, 1999, http://csrc.nist.gov/fips/fips46-3.pdf.

[4]. A. J. Menezes, P.C. van Oorschot, and S.A. Vanstone, *Handbook of Applied Cryptography* (CRC Press Series on Discrete Mathematics and Its Applications), 1996.

[5]. NIST, "Commerce Department Announces Winner of Global Information Security Competition," October 2, 2000, http://www.nist.gov/public_affairs/releases/g00-176.htm 或 http://www.nist.gov/aes/.

[6]. J. Demen and V. Rijmen, "The Rijndael Block Cipher," Document version 2, March 1999, http://www.esat.kuleuven.ac.be/~rijmen/rijndael.

[7]. NIST, Draft FIPS for the Advanced Encryption Standard (AES), http://csrc.nist.gov/publications/drafts/dfips-AES.pdf, February 28, 2001.

[8]. "New European Schemes for Signatures, Integrity, and Encryption (NESSIE), " http://www.cosic.esat.kuleuven.ac.be/nessie/.

[9]. "Call for Cryptographic Techniques," IPA, June 2000, http://www.ipa.go.jp/security/enc/CRYPTREC/index-e.html.

[10]. R.L. Rivest, M.J.B. Robshaw, R. Sidney, and Y.L. Yin, "The RC6 Block Cipher," August 1998. ftp://ftp.rsasecurity.com/ pub/rsalabs/rc6/rc6v11.pdf.

[11]. H. Ohtsuka and H. Ueda: "Software Implementation of FEAL-NX", ISEC2000-70, Vol. 100, No. 324, pp.53-70, Sept. 2000. 參見 http://info.isl.ntt.co.jp/feal-nx/.

[12]. K. Aoki, T. Ichikawa, M. Kanda, M. Matsui, S. Moriai, J. Nakajima, and T. Tokita, "Camellia - A 128-Bit Block Cipher Suitable for Multiple Platforms," *7th Annual Workshop on Selected Areas in Cryptography (SAC2000)*, August 2000. 參見 http://info.isl.ntt.co.jp/camellia/.

[13]. *Hitachi Single-Chip Microcomputer H8/3113 Hardware Manual*, Hitachi Ltd., 1998. 參見 http://www.hitachi.co.jp/Sicd/English/Products/micom/ 300micome.htm.

[14]. *MC68HC05B4/705B5/05B6/05B8/(7)05B16/705B16N/(7)05B32 Technical Data*, Rev. 4, Motorola Ltd., January 1999. 參見 http:// www.mcu.motsps.com/.

[15]. G. Keating, "Performance Analysis of AES candidates on the 6805 CPU core," *Second AES Candidate Conference (AES2)*, 1999. 參見 http://csrc.nist.gov/encryption/aes/round1/conf2/papers/keating.pdf 或 http://www.ozemail.com.au/%7Egeoffk/aes-6805/.

[16]. G. Hachez, F. Koeune, and J.-J. Quisquater, "cAESar results: Implementation of Four AES Candidates on Two Smart Cards," *Second AES Candidate Conference (AES2)*, 1999. 參見 http://csrc.nist.gov/encryption/aes/round1/conf2/papers/hachez.pdf.

[17]. John Kelsey, Bruce Schneier, and David Wagner, "Key-schedule cryptanalysis of IDEA, G-DES, GOST, SAFER, and triple-DES," *CRYPTO '96*, pp. 237-251, 1996..

附錄一：

以下我們列出AES-128於日立公司智慧卡硬體模擬器及摩托羅拉公司硬體模擬器執行之實際結果。測試所用的資料係採用AES草案[7]附錄B、C的範例。

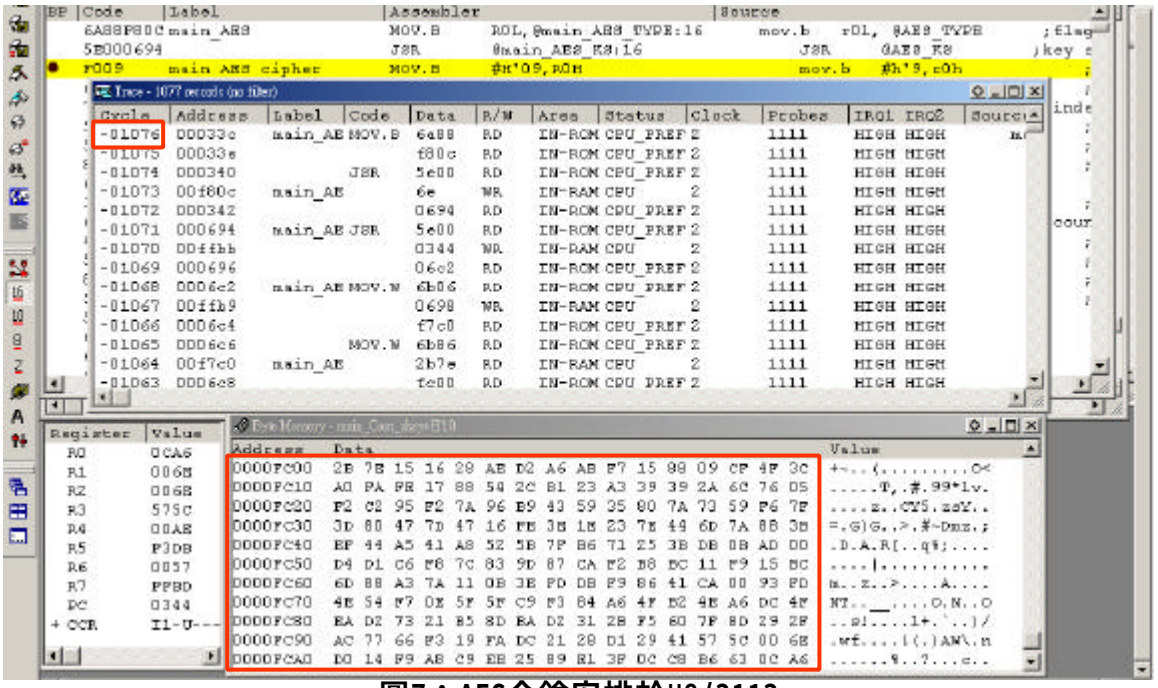

圖7：AES金鑰安排於H8/3113

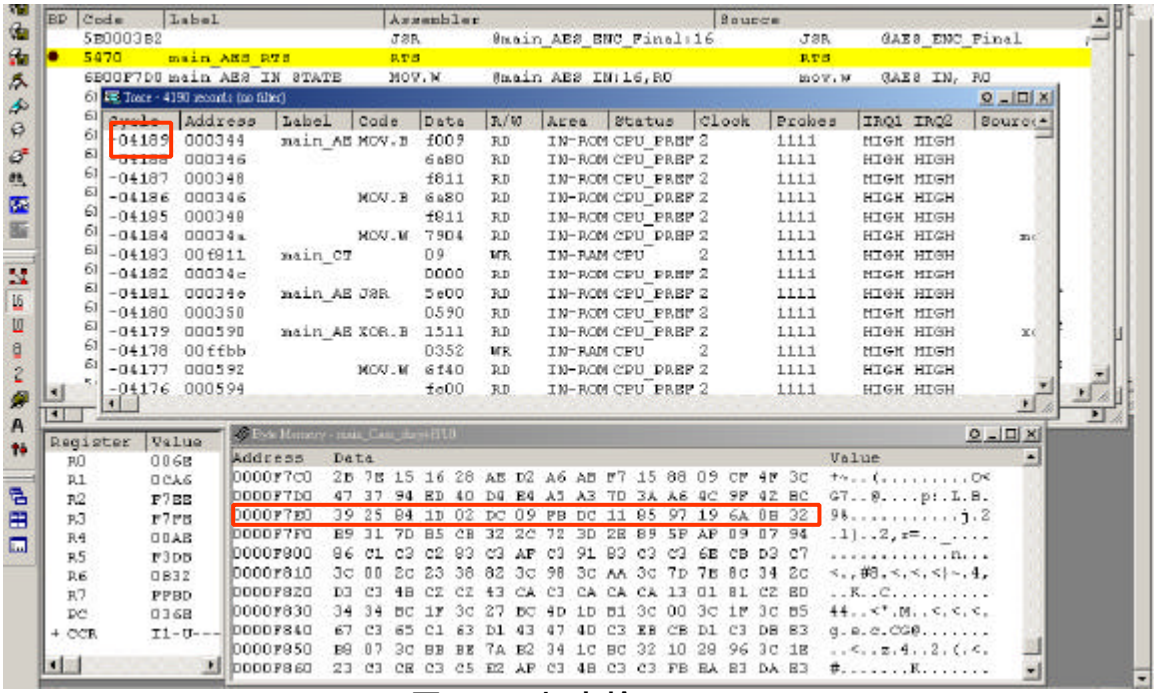

圖8：AES加密於H8/3113

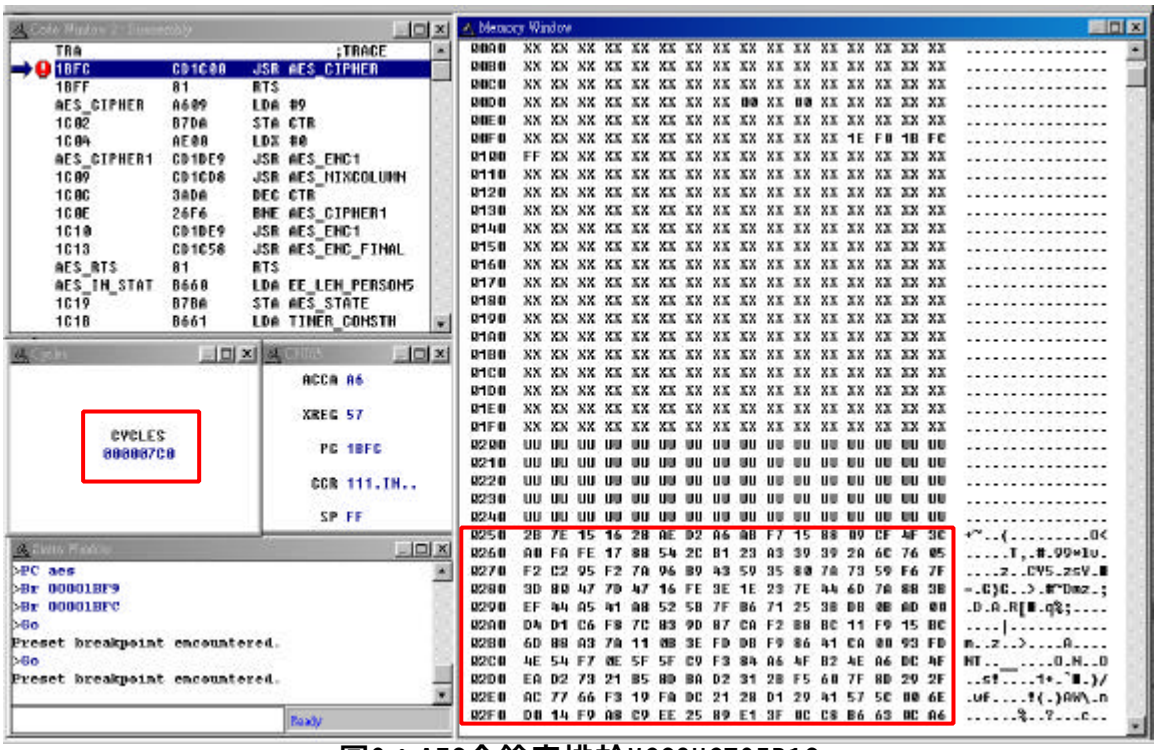

圖9：AES金鑰安排於MC68HC705B16

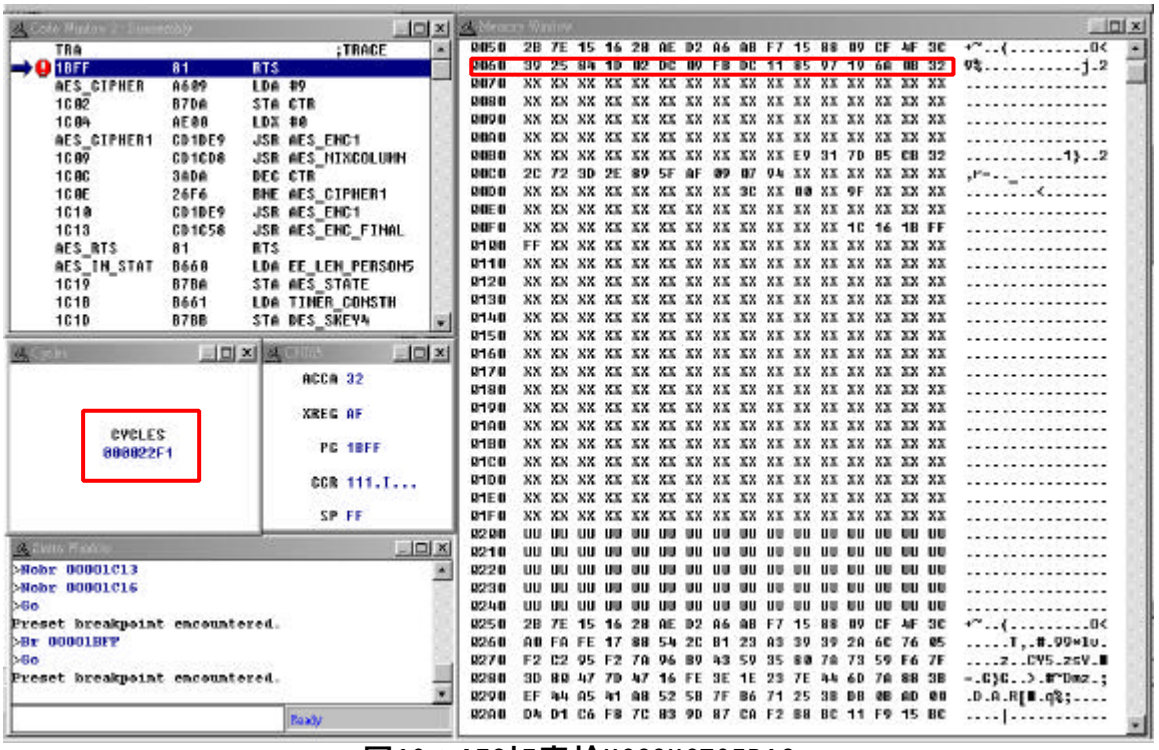

圖10：AES加密於MC68HC705B16

更詳盡的硬體模擬資料請參見網頁http://www.nkfust.edu.tw/~chyang/isc2001/.